



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/707,191	11/25/2003	Terry M. Olkin	60468.300204	1190

32112759006/29/2007
INTELLECTUAL PROPERTY LAW OFFICES
1901 S. BASCOM AVENUE, SUITE 660
CAMPBELL, CA 95008

EXAMINER
GELAGAY, SHEWAYE

ART UNIT
2137

PAPER NUMBER

MAIL DATE
06/29/2007

DELIVERY MODE
PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

Office Action Summary	Application No.	Applicant(s)	
	10/707,191	OLKIN ET AL.	
	Examiner	Art Unit	
	Shewaye Gelagay	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 08 March 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-27 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-27 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>3/8/07</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. This office action is in response to Applicant's amendment filed on March 8, 2007. Claims 1-27 are pending.

Information Disclosure Statement

2. In view of the amendment filed March 8, 2007, the Examiner withdraws the objection to the IDS.

Claim Rejections - 35 USC § 112

3. In view of the amendment filed March 8, 2007, the Examiner withdraws the rejection of claims 1, 5, 14, 19, 23 and 26 under 35 U.S.C. 112.

Response to Arguments

4. Applicant's argument filed March 8, 2007 regarding the rejection of claims 1, 5, 14, 19, 23 and 26 under 35 USC 102 (b) is persuasive and therefore the rejection has been withdrawn. The rest of applicant's argument have been fully considered but they are not persuasive. In response to the arguments concerning the previously rejected claims, the following comments are made:

The applicant argued that Andivahis does not use an authentication assertion (i.e. an already existing assertion issued by an authority) and applicant's source does not need to send a message to a key server to get a supply of random bit strings that

Art Unit: 2137

only that key server can then recognize. Andivahis teaches prior to any action authentication process takes place between the sender and the key server, the type of authentication information is preferably included with each message sent by the sender to the Key Server. (col. 4, lines 22-37) In addition, Andivahis teaches registering a user using a personal identifying information using additional credentials, such as public key certificate, an ITU X.509 certificate or the like, the credentials can be used in the future to determine which features of the system a user may access. A user uses certificates and submits the public key encryption key to the Key Server and the Key Server updates its database with the new user's information and corresponding credential. Thereafter, the Key Server can use the credential information to determine which registered user has requested a specific encryption or decryption key, and which services that user has requested. (col. 13, lines 13-62) Therefore, Andivahis teaches authenticating a user not only with email address but also by other credentials such as certificate (i.e. equivalent to the assertion)

Applicant argued that Andivahis is not teaching the use of an authentication assertion. Applicant argued that "The cite states the sender is authenticated," but the distinction between being authenticated and doing that with an authentication assertion has apparently been missed." Andivahis teaches a user can register using personal identifying information and using additional credentials such as certificate (i.e. equivalent to assertion)

The applicant argued that how Andivahis does not teach storing information from said source authentication assertion. The Examiner would like to point out Andivahis

Art Unit: 2137

teaches registering a user using a personal identifying information using additional credentials, such as public key certificate, an ITU X.509 certificate or the like, the credentials can be used in the future to determine which features of the system a user may access. (col. 13, lines 13-62)

The applicant argued that there is nothing in the cite that is equivalent to a second request, or one specifically for a decryption key. The Examiner would like to point out that Andivahis teaches after the recipient and the key server establish a communication link and the recipient is authenticated, the recipient sends a key retrieval request. (col. 6, lines 24-33)

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., "an already existing assertion issued by an authority", "whole keys") are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

The applicant argued that Andivahis does not teach a request that includes an authentication assertion. The examiner disagrees. (see previous discussion above). Andivahis does not explicitly teach a first request for a transaction identifier that includes an authentication assertion. Favazza teaches a customer inserting an assertion, and a signature into an initial request to a web service. (page 1, paragraphs 9-10) Therefore it would have been obvious to one ordinary skill in the art to modify the method disclosed by Andivahis with Favazza in order to have a system that enables sharing information in

Art Unit: 2137

a secure environment by utilizing assertions that are embedded in transport and messaging networks. (page 1, paragraphs 6 and 7; Favazza)

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Andivahis et al. (hereinafter Andivahis) U.S. Patent Number 7,146,009 in view of Favazza et al. (hereinafter Favazza) U.S. Publication Number 2004/0139319.

As per claims 1, 5, 14, 19, 23 and 26:

Andivahis teaches a method for a transaction source and a transaction target to exchange a transaction that cannot be repudiated, the method comprising:

(a) receiving a request for a transaction identifier to identify the transaction, wherein said request includes a source authentication assertion; (col. 4, lines 22-37)

(b) verifying said source authentication assertion; (col. 4, lines 40-45)

(c) storing said transaction identifier and information from said source authentication assertion, thereby establishing information making the transaction source unable to plausibly repudiate once it encrypts and sends the transaction; (col. 4, lines 61-col. 5, line 9)

(d) providing said transaction identifier in reply to said request so that the transaction and said transaction identifier can be sent to the transaction target; (col. 4, lines 61-col. 5, line 9)

(e) receiving a second request for a decryption key to decrypt the transaction once it has been received by the transaction target, wherein said second request includes said transaction identifier and a target authentication assertion; (col. 6, lines 24-29)

(f) verifying said target authentication assertion; (col. 6, lines 45-49)

(g) storing information from said target authentication assertion with the transaction identifier; (col. 6, lines 50-67) and

(h) providing said decryption key in reply to said second request so that the transaction can be decrypted, thereby establishing information making the transaction target unable to plausibly repudiate being a recipient of the transaction. (col. 6, lines 50-67)

Andivahis does not explicitly disclose receiving a first request includes an authentication assertion. Favazza in analogous art, however, discloses a first request includes an authentication assertion. (page 1, paragraphs 9 and 10) Therefore it would have been obvious to one ordinary skill in the art to modify the method disclosed by

Andivahis with Favazza in order to have a system that enables sharing information in a secure environment by utilizing assertions that are embedded in transport and messaging networks. (page 1, paragraphs 6 and 7; Favazza)

As per claims 2, 6, 20 and 24:

The combination of Andivahis and Favazza teaches all the subject matter as discussed above. In addition, Andivahis further discloses a method wherein said step (d) includes also providing an encryption key to encrypt the transaction. (col. 4, lines 61-col. 5, line 9)

As per claims 3, 7, 9, 12, 21 and 25:

The combination of Andivahis and Favazza teaches all the subject matter as discussed above. In addition, Andivahis further discloses a method the method further comprising: (i) receiving an information request for source information about the transaction source, wherein said information request includes said transaction identifier; (j) retrieving at least some of said information from said source authentication assertion stored in said step (c) with said transaction identifier and determining said source information therefrom; and (k) providing said source information in reply to said information request. (col. 6, lines 57-67; col. 18, lines 25-67)

As per claims 4 and 22:

The combination of Andivahis and Favazza teaches all the subject matter as discussed above. In addition, Andivahis further discloses a method comprising: (i) receiving an information request for target information, wherein said information request includes said transaction identifier and information identifying the transaction

Art Unit: 2137

target; (j) determining if said information identifying the transaction target matches with any said information from said target authentication assertion stored with the transaction identifier stored in said step (g) and determining said target information therefrom; and (k) providing said target information in reply to said information request. (col. 18, lines 25-67)

As per claims 10 and 16:

The combination of Andivahis and Favazza teaches all the subject matter as discussed above. In addition, Andivahis further discloses a method wherein: said step (c) includes also storing a decryption key usable to decrypt the transaction; and said step (g) includes also providing said decryption key, thereby facilitating decryption of the transaction by a party making said information request even when said party is not the transaction source or a target of the transaction. (col. 4, line 46-col. 6, line 15)

As per claims 11 and 17:

The combination of Andivahis and Favazza teaches all the subject matter as discussed above. In addition, Andivahis further discloses a method wherein: said information request received in said step (e) also includes the transaction; and said step (g) includes decrypting the transaction before providing said source information in reply to said information request. (col. 4, line 46-col. 6, line 15)

As per claims 13 and 18:

The combination of Andivahis and Favazza teaches all the subject matter as discussed above. In addition, Favazza further discloses a method wherein said step (g) includes also providing the transaction in decrypted form in said reply to said

Art Unit: 2137

information request, thereby facilitating a party making said information request being able to confirm the content of the transaction even when said party is not the transaction source or a target of the transaction. (page 3, paragraphs 40-43)

As per claim 15 and 27:

The combination of Andivahis and Favazza teaches all the subject matter as discussed above. In addition, Andivahis further discloses a method comprising: (e) receiving an information request for target information, wherein said information request includes said transaction identifier and information identifying the transaction target; (f) retrieving at least some of said information from said target authentication assertion stored in said step (c) with said transaction identifier and determining said target information therefrom; and (g) providing said target information in reply to said information request. (col. 18, lines 25-67)

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

Art Unit: 2137

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

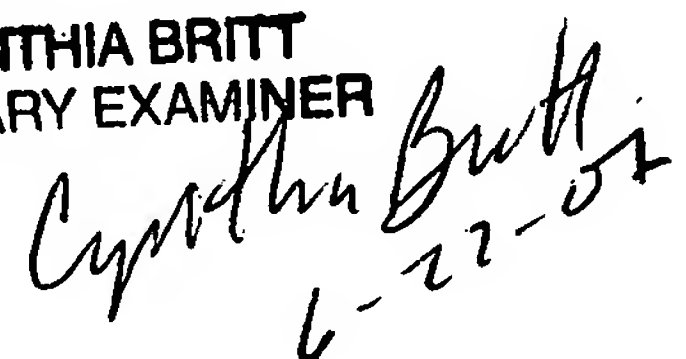
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shewaye Gelagay



CYNTHIA BRITT
PRIMARY EXAMINER



6-22-02